ESTUDOS PRELIMINARES

I – ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1 ESPECIFICAÇÃO DOS REQUISITOS

1.1 DE NEGÓCIO

1.1.1 A solução deverá:

1.1.1.1 Permitir a gestão de vulnerabilidades em sistemas operacionais.

1.1.1.1.1 Testar os *hosts* (físicos e virtuais), comparando as bases de dados de vulnerabilidades mantidas por organizações especializadas em segurança da informação e por grandes fabricantes de *software*.

1.1.1.2 Permitir a gestão de vulnerabilidades em sistemas e páginas *web*.

1.1.1.2.1 Testar as aplicações e páginas *web*, internas e externas, comparando as bases de dados de vulnerabilidades mantidas por organizações especializadas em segurança da informação e por grandes fabricantes de *software*.

1.1.1.3 Ser capaz de emissão de relatórios dos testes realizados, das vulnerabilidades encontradas e de sua correção, necessários ao acompanhamento das atividades de identificação, análise, priorização e mitigação de riscos.

1.1.2 Atualmente existe a necessidade de aquisição de ferramenta de gestão de vulnerabilidades, conforme abaixo:

Item	Descrição	Tipo
1	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações	Ativos de rede
2	Licenciamento para solução de análise dinâmica	Aplicações *Web*
3	Serviço de instalação e configuração da solução	-
4	Repasse tecnológico	Por um período mínimo de 20 (vinte) horas
5	Suporte técnico	04 (quatro) horas de serviço especializado

1.2 DE CAPACITAÇÃO

1.2.1 Haverá necessidade de treinamento ou repasse tecnológico, presencial ou a distância, no mínimo de **20 (vinte) horas**, visando capacitar os servidores da Secretaria de Tecnologia da Informação e Eleições (STIE) no uso da ferramenta.

1.3 LEGAIS

1.3.1 A contratação obedecerá às regras gerais de fornecimento ao Poder Público, inexistindo requisitos legais específicos para essa contratação.

1.4 MANUTENÇÃO

1.4.1 Suporte técnico deve estar disponível durante a vigência de uso da licença.

1.4.2 Atualizações da solução disponível durante a vigência de uso da licença.

1.5 TEMPORAIS

1.5.1 A fornecedora da solução terá até **05 (cinco) dias** contados após a formalização da contratação para fornecer os *softwares* ou as subscrições contratadas.

1.6 DE SEGURANÇA

1.6.1 A fornecedora da solução deverá obedecer aos critérios, padrões, normas e procedimentos operacionais adotados pela JUSTIÇA ELEITORAL, em especial:

1.6.1.1 O fornecedor assinará, no ato da entrega das licenças e do serviço, Termo de Confidencialidade, em que se comprometerá a não acessar, não divulgar e proteger todos os dados de infraestrutura e de vulnerabilidades do contratante a que tiver acesso, que abrangerá todos os seus colaboradores e terceiros, sob as penas da lei.

1.6.1.2 Da gestão de ativos.

1.6.1.3 Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse da JUSTIÇA ELEITORAL ou de terceiros de que tomar conhecimento em razão da execução do objeto desta contratação devendo orientar seus funcionários nesse sentido.

1.6.1.4 Submeter seus recursos técnicos aos regulamentos de segurança e disciplina instituídos pela JUSTIÇA ELEITORAL, durante o tempo de permanência nas suas dependências, observando a Portaria 226/2018-GP-TRE/RN, que dispõe sobre as medidas de controle de acesso, circulação e permanência de pessoas nos prédios do Edifício-Sede do TRE/RN, do Centro de Operações da Justiça Eleitoral (COJE), Fórum Eleitoral de Natal e, no que couber, aos prédios das Zonas Eleitorais do Interior do Estado.

1.7 SOCIAIS, AMBIENTAIS E CULTURAIS

1.7.1 É de responsabilidade da empresa fornecedora da solução a disposição final responsável e ambientalmente adequada das embalagens e materiais que porventura venham a ser utilizados em observância à Logística Reversa disposta no art. 33 da Lei Nº 12.305/2010, que institui a Política Nacional de Resíduos Sólidos.

1.7.2 O TRE/RN reserva-se o direito de assumir a responsabilidade a que se refere o item anterior, podendo dar outra destinação às embalagens e materiais após o uso, caso julgue mais conveniente para a Administração.

1.7.3 Qualquer material que venha a ser utilizado na embalagem dos produtos ofertados e/ou utilizados na execução dos serviços deverão ter sua reciclabilidade efetiva no Brasil.

1.8 DE ARQUITETURA TECNOLÓGICA

1.8.1 Tendo como base os requisitos funcionais definidos, foram identificados os seguintes requisitos tecnológicos:

1.8.1.1 A solução deve estar licenciadas e inclusas todas as funcionalidades para realizar varreduras *(scans)* de vulnerabilidades, avaliação de configuração e conformidade *(baseline e compliance)*, indícios e padrões de códigos maliciosos conhecidos *(malware)* para, no mínimo, 250 (duzentos e cinquenta) *IPs*.

1.8.1.2 A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede.

1.8.1.3 A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de *IoT*.

1.8.1.4 A solução deve ser capaz de identificar no mínimo 50.000 (cinquenta mil) *CVEs (Common Vulnerabilities and Exposures).*

1.8.1.5 A solução deve ter a capacidade de adicionar etiquetas *(tags)* aos ativos de maneira automática, manual e possibilitar o uso de regras com parâmetros específicos para aplicação das mesmas.

1.8.1.6 A solução deve atribuir a todas as vulnerabilidades uma severidade baseada no *CVSSv3 score*.

1.8.1.7 A solução deve calcular a criticidade com base nos dados agregados e consolidados do ativo, dados de segurança, sistema e conformidade, bem como hierarquias e prioridades.

1.8.1.8 A solução deve fornecer criptografia de ponta a ponta dos dados de vulnerabilidades.

1.8.1.9 A solução deve possuir a capacidade de armazenar informações dos ativos descobertos no ambiente.

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

1.8.1.10 A solução deve possuir um sistema de busca de informações de um determinado ativo com, no mínimo, as seguintes características:

1.8.1.10.1	Por sistema operacional
1.8.1.10.2	Por um determinado software instalado
1.8.1.10.3	Por ativos impactados por uma determinada vulnerabilidade

1.8.1.11 A solução deve possuir suporte para a adição de detecções personalizadas usando o OVAL *(Open Vulnerability Assessment Language).*

1.8.1.12 A solução deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente.

1.8.1.13 A solução deve possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual.

1.8.1.14 A solução deve possuir um sistema de pontuação e priorização das vulnerabilidades.

1.8.1.15 A solução deve ser capaz de aplicar algoritmos de aprendizagem de máquina *(machine learning)* para analisar as características relacionadas a vulnerabilidades.

1.8.1.16 O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:

1.8.1.16.1	*CVSSv3 Impact Score*
1.8.1.16.2	Idade da Vulnerabilidade
1.8.1.16.3	Se existe ameaça ou *exploit* que explore a vulnerabilidade
1.8.1.16.4	Número de produtos afetados pela vulnerabilidade

1.8.1.17 A solução deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra vulnerabilidades encontradas, incluindo *feeds* de inteligência de ameaças ao vivo.

1.8.1.18 A solução deve possuir uma *API* para automação de processos e integração com aplicações terceiras permitindo, no mínimo, a extração de dados para carga no *SIEM*.

1.8.1.19 A solução deve possuir uma API para automação de processos e integração com aplicações *ITSM* do órgão para as vulnerabilidades encontradas, permitindo o agrupamento no chamado por ações corretivas.

1.8.1.20 A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional.

1.8.1.21 Se for baseada em nuvem, a solução deve possuir conectores para, no mínimo, as seguintes plataformas:

1.8.1.21.1	*Amazon Web Service (AWS)*
1.8.1.21.2	*Microsoft Azure*
1.8.1.21.3	*Google Cloud Platform*

1.8.1.22 A solução deve ser capaz de produzir relatórios nos seguintes formatos: *PDF, CSV* ou *HTML*.

1.8.1.23 A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados.

1.8.1.24 A solução deve ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o monitoramento em tempo real.

1.8.1.25 A solução deve possuir sensores, no mínimo, com as seguintes funcionalidades:

1.8.1.25.1	Execução de verificação completa do sistema (rede), adequada para qualquer *host*
1.8.1.25.2	Verificação sem recomendações da rede, para que se possa personalizar totalmente as configurações da verificação
1.8.1.25.3	Autenticação de *hosts* e enumeração de atualizações ausentes
1.8.1.25.4	Execução de varredura simples para descobrir *hosts* ativos e portas abertas
1.8.1.25.5	Utilização de um *scanner* para verificar aplicativos da web
1.8.1.25.6	Avaliação de dispositivos móveis
1.8.1.25.7	Auditoria de configuração de serviços em nuvem de terceiros
1.8.1.25.8	Auditoria de configuração dos gerenciadores de dispositivos móveis
1.8.1.25.9	Auditoria de configuração dos dispositivos de rede
1.8.1.25.10	Auditoria de configurações do sistema em relação a uma linha de base conhecida
1.8.1.25.11	Detecção de desvio de segurança *Intel AMT*
1.8.1.25.12	Verificação de *malware* nos sistemas *Windows* e *Unix*

1.8.1.26 A solução deve ser possível determinar em tempo real, quais portas de serviços (*UDP/TCP*) estão abertas em determinado ativo.

1.8.1.27 A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para no mínimo:

1.8.1.27.1	Bancos de dados
1.8.1.27.2	*Hypervisors* (no mínimo VMWare ESX/ESXi)
1.8.1.27.3	Dispositivos móveis
1.8.1.27.4	Dispositivos de rede
1.8.1.27.5	*Endpoints*
1.8.1.27.6	Aplicações

1.8.1.28 A solução deve ser capaz de em tempo real detectar *logins* e *downloads* de arquivos em um compartilhamento de rede.

1.8.1.29 A solução deve permitir identificar vulnerabilidades associadas a servidores *SQL* no tráfego de rede.

1.8.1.30 A solução deve possuir interface para integração com as principais soluções de *SIEM* de mercado,

tais como *IBM QRadar, Microfocus ArcSight e Splunk.*

1.8.1.31 A solução deve possibilitar a realização de cópias de segurança, funcionamento em alta disponibilidade e criptografia de todos os dados armazenados, além de incluir todo o software e licenciamento necessários para o funcionamento completo de acordo com as funcionalidades previstas neste Termo de Referência.

1.8.1.32 A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.

1.8.1.33 Configuração de segurança e acesso à gerência da solução:

1.8.1.33.1	Todos os dados armazenados nos servidores da solução devem ser criptografados e possuir logs de acesso
1.8.1.33.2	Os dados em trânsito devem usar ao menos o algorítimo *TLS* 1.2 de chave 2048 *bits*
1.8.1.33.3	Os dados em trânsito devem ser criptografados ao menos com o algorítimo *AES*-128 *bits*
1.8.1.33.4	Os algorítimos de *hash* devem usar ao menos o algorítimo *SHA*-256
1.8.1.33.5	Será aceito como comprovação critérios de criptografia publicação em site do fabricante ou declaração do próprio fabricante
1.8.1.33.6	Os dados armazenados devem ser criptografados ao menos com o algorítimo *AES*-256 *bits*
1.8.1.33.7	Somente servidores do TRE/RN ou pessoa por ela autorizada poderão ter acesso aos dados da solução
1.8.1.33.8	A solução deve permitir a criação de, no mínimo, 20 (vinte) contas para gerência e acesso aos relatórios, sem custo adicional
1.8.1.33.9	A empresa fornecedora da solução não deverá ter acesso a rede interna da contratante e todo trafego de dados deverá ser de saída e iniciado pelos *scanners (on-premises*)

1.8.1.34 Todas as licenças de uso de *software* devem ser registradas, na data da entrega, em nome do TRE/RN no site do fabricante.

1.8.1.35 Dos Relatórios:

1.8.1.35.1	Deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como a geração de relatórios sob demanda
1.8.1.35.2	A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção de todos os ativos existentes
1.8.1.35.3	A solução deve suportar a criação de relatórios criptografados (protegidos por senha configurável)
1.8.1.35.4	A solução deve suportar o envio automático de relatórios para destinatários específicos
1.8.1.35.5	A solução deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual
1.8.1.35.6	A solução deve permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos
1.8.1.35.7	A solução deve fornecer relatórios do tipo "*scorecard*" para as partes interessadas da empresa
1.8.1.35.8	A solução deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: grupo de ativos, usuários e vulnerabilidades

1.8.1.36 A solução deve permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas.

1.8.1.37 A solução deve possuir ou permitir a criação de relatórios com as seguintes informações:

1.8.1.37.1	*Hosts* verificados sem credenciais
1.8.1.37.2	*Top* 100 Vulnerabilidades mais críticas
1.8.1.37.3	*Top* 10 *Hosts* infectados por *Malwares*
1.8.1.37.4	*Hosts* exploráveis por *Malwares*
1.8.1.37.5	Total de vulnerabilidades que podem ser exploradas pelo *Metasploit*
1.8.1.37.6	Vulnerabilidades críticas e exploráveis
1.8.1.37.7	Máquinas com vulnerabilidades que podem ser exploradas

1.8.1.38 A solução deve possuir *dashboards* customizáveis onde o administrador pode criar, editar ou remover painéis de acordo com a necessidade.

1.8.1.39 A solução deve ser capaz de inventariar todos os ativos da rede local e publicados na Internet, sem limites de endereços *IPs*.

1.8.1.40 A plataforma de *software* deve ser capaz de realizar varreduras (*scans*) de vulnerabilidades para no mínimo 250 Ips.

1.8.1.41 A plataforma de *software* deve ser licenciada para um número ilimitado de *scanners* (prevendo redundância).

1.8.1.42 A solução deve permitir a configuração de vários painéis e *widgets*.

1.8.1.43 A solução deve ser capaz de medir e reportar ameaças.

1.8.1.44 A solução deve ser capaz de visualizar ameaças críticas ao ambiente monitorado.

1.8.1.45 A plataforma de software deve realizar varreduras em uma variedade de sistemas operacionais, suportando pelo menos *hosts* baseados em *Windows, Linux* e *Mac OS*, bem como *appliances* virtuais.

1.8.1.46 A plataforma de *software* deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central.

1.8.1.47 A plataforma de *software* deve fornecer agentes instaláveis em sistemas operacionais, pelo menos *Windows, Linux* e *Mac OS*, para o monitoramento contínuo de configurações e vulnerabilidades.

1.8.1.48 A plataforma de software deve permitir o monitoramento através de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.

1.8.1.49 A plataforma de *software* deve permitir o monitoramento sem a necessidade de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.

1.8.1.50 A plataforma de *software* deve incluir a capacidade de programar períodos de tempo e data onde varreduras não podem ser executadas, por exemplo em determinados dias do mês ou

determinados horários do dia.

1.8.1.51 No caso onde uma atividade de varredura seja interrompida por invadir o período não permitido, o mesmo deve ser capaz de ser reiniciado de onde parou.

1.8.1.52 A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura.

1.8.1.53 A plataforma de *software* deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (*LDAP* e *Active Directory)* e *root* para sistemas *Linux*.

1.8.1.54 A plataforma de *software* deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo.

1.8.1.55 A plataforma de *software* deve ser capaz de realizar pesquisas de dados confidenciais.

1.8.1.56 A solução deve possuir módulo para realizar análise dinâmica em aplicações *Web*:

1.8.1.56.1	A solução deve possuir módulo para realizar varreduras de vulnerabilidades para, no mínimo, 05 (cinco) aplicações *Web*, cobrindo no mínimo, mas não limitando-se a base de ameaças apontadas pelo *OWASP Top 10, CWE* e *WASC*
1.8.1.56.2	A solução de análise deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações *Web*
1.8.1.56.3	A solução de análise deverá ser capaz de executar varreduras em sistemas *Web* através de seus endereços *IPs* ou *FQDN* (*DNS*)
1.8.1.56.4	A solução de análise deve ser capaz de identificar vulnerabilidades de divulgação de dados, como vazamento de informações de identificação pessoal
1.8.1.56.5	Para varreduras do tipo extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos: a) *Cookies*, *headers*, formulários e *links* b) Nomes e valores de parâmetros da aplicação c) Elementos *JSON* e *XML* d) Elementos *DOM*
1.8.1.56.6	A solução deverá também permitir a execução da função *crawler*, que consiste na navegação para descoberta das *URLs* existentes na aplicação
1.8.1.56.7	A solução de análise deve suportar a integração com o softwares de automação de testes para permitir sequências de autenticação complexas
1.8.1.56.8	A solução de análise deve ser capaz de realizar testes/varreduras em aplicações separadas, simultaneamente limitadas ao número de licenças
1.8.1.56.9	A solução de análise deve oferecer suporte à capacidade de testar novamente a vulnerabilidade específica que foi detectada anteriormente no aplicativo *Web*
1.8.1.56.10	A solução deve ser capaz de utilizar scripts customizados de *crawling* com parâmetros definidos pelo usuário
1.8.1.56.11	A solução deve ser capaz de excluir determinadas *URLs* da varredura através de expressões regulares
1.8.1.56.12	A solução deve ser capaz de excluir determinados tipos de arquivos através de suas extensões

1.8.1.56.13	A solução deve ser capaz de instituir no mínimo os seguintes limites: a) Número máximo de *URLs* para crawling e navegação b) Número máximo de diretórios para varreduras c) Número máximo de elementos *DOM* d) Tamanho máximo de respostas e) Tempo máximo para a varredura f) Número máximo de conexões *HTTP(S)* ao servidor hospedando a aplicação *Web* g) Número máximo de requisições *HTTP(S)* por segundo
1.8.1.56.14	A solução deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual
1.8.1.56.15	A solução deve suportar o envio de notificações por email
1.8.1.56.16	A solução deverá ser compatível com avaliação de web services *REST* e *SOAP*
1.8.1.56.17	A solução de análise deve suportar os seguintes esquemas de autenticação: Autenticação Básica (*Digest*). *NTLM*. Autenticação de *Cookies*
1.8.1.56.18	A solução deve ser capaz de importar scripts de autenticação previamente configurados pelo usuário
1.8.1.56.19	A solução de análise deve ser capaz de exibir os resultados das varreduras de forma temporal para acompanhamento de correções e introdução de novas vulnerabilidades
1.8.1.56.20	Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações
1.8.1.56.21	Para cada vulnerabilidade encontrada, deve ser exibido detalhes e evidências
1.8.1.56.22	Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação

1.8.1.56.23	Serviço de Detecção de *Malware*: a) A solução de análise deve utilizar a plataforma de gerenciamento de vulnerabilidades existente b) A solução de análise deve permitir visualizar o acompanhamento das atividades de verificação, páginas infectadas e tendências de infecção por *malware* c) A solução de análise deve fornecer relatórios de resumo geral de todas as aplicações web e resumo de uma aplicação específica, que serão exportados para os formatos *XML, HTML ou PDF*
1.8.1.56.24	A solução deve ser capaz de realizar varreduras nos seguintes componentes/aplicações: ○ *WordPress* ○ *IIS 6.x e IIS 10.x* ○ *ASP 6* ○ *NET 2* ○ *Apache HTTPD 2.2.x e 2.4.x* ○ *Tomcat 6.x, 7.x, 8.x e superiores* ○ *Jetty 8 e superiores* ○ *Nginx* ○ *PHP 5.3.x, 5.4.x, 5.6.x, 7.0.x e 7.1.x e superiores* ○ *Java 1.5, 1.6, 1.7 e 1.8 e superiores* ○ *Jboss 4.x e 7.x e superiores* ○ *WildFly 8 e 10 e superiores* ○ *Plone 2.5.x e 5.2.1.41.x e superiores* ○ *Zope* ○ *Python 2.4.4 e superiores* ○ *J2EE* ○ *Ansible* ○ *Joomla* ○ *Moodle* ○ *Docker Conteiner* ○ *Elk* ○ *GIT* ○ *Grafana* ○ *Redmine*

1.9 DE PROJETO E DE IMPLEMENTAÇÃO

1.9.1 Não se aplica.

1.10 DE IMPLANTAÇÃO

1.10.1 O serviço de implantação poderá ser executado presencialmente na Sede do TRE/RN ou remotamente, acompanhados e supervisionados por sua equipe técnica e realizados prioritariamente durante o expediente normal da Justiça Eleitoral do Rio Grande do Norte.

1.10.1.1 Caso necessário, visando minimizar o impacto para os usuários, o TRE/RN poderá exigir a execução da implantação fora do horário de expediente normal, ou seja, durante a noite, a madrugada ou em finais de semana e feriado.

1.11 DE GARANTIA E MANUTENÇÃO

1.11.1 Os softwares e licenças fornecidos deverão estar cobertos por garantia que ofereça atualizações necessárias para a correção de vícios, pelo período especificado no termo de referência, a contar da data do aceite provisório do software, conforme Art. 73, I, "a", da Lei 8.666/1993.

1.11.1.1 O suporte pelo fabricante será obrigatório.

1.11.1.2 O suporte pela fornecedora da solução será opcional e ela poderá subcontratar uma empresa autorizada pelo fabricante para prestar o suporte técnico de primeiro nível.

1.11.2 Devem estar explícitos na proposta os *part numbers* de garantia oficial do fabricante no Brasil.

1.11.3 O tempo da garantia e suporte técnico estarão explicitadas nas especificações específicas dos respectivos itens.

1.11.4 A empresa deve indicar, na assinatura do contrato, os procedimentos para abertura de suporte técnico, cabendo a este órgão a abertura do chamado com intermediação da empresa fornecedora dos produtos ou diretamente com o fabricante.

1.11.5 A empresa deve possuir, no momento da assinatura do contrato, pelo menos **01 (um)** profissional com certificação técnica emitida pelo fabricante, capaz de prestar o serviço especializado de instalação e configuração da solução.

1.11.6 Os chamados telefônicos deverão estar disponibilizados de segunda à sexta-feira, das 8 às 18 horas, adotando-se para tanto o horário de Brasília.

1.11.6.1 O tempo para a resposta dos chamados dependerá da severidade do problema conforme abaixo:

1.11.6.1.1 Não poderá ser superior a **02 (duas) horas**, após abertura do chamado, para problemas com severidade crítica (funcionalidade do produto completamente degradada, impacto crítico nas operações).

1.11.6.1.2 Não poderá ser superior a **12 (doze) horas**, após abertura do chamado, para problemas com severidade alta (funcionalidade do produto severamente degradada, impacto severo nas operações).

1.11.6.1.3 Não poderá ser superior a **02 (dois) dias úteis**, após abertura do chamado, para problemas com severidade média (erros, problemas gerais, produto danificado, no entanto, as operações permanecem funcionais).

1.11.7 A empresa fornecedora da solução ou o fabricante deverão disponibilizar, cumulativamente, abertura de suporte técnico por meio de atendimento telefônico, *website e e-mail.*

1.11.8 Os serviços de garantia aos produtos deverão ser prestados por empresa credenciada pelo fabricante ou pelo próprio fabricante dos produtos fornecidos.

1.11.9 A fornecedora da solução ou o fabricante deverão disponibilizar um portal web com disponibilidade de 24 (vinte e quatro) horas por dia, 07(sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano, com sistema de *help-desk* para abertura de chamados de suporte técnico.

1.11.10 A equipe técnica do TRE/RN poderá abrir, gerenciar status e conferir todo o histórico de chamados de suporte técnico, mediante *login* e senha de acesso ao sistema.

1.11.11 Os chamados abertos por e-mail deverão ter sua abertura automática no portal *web*.

1.11.12 Todo o chamado aberto deverá ter sua resolução técnica registrada no sistema *web* de *help-desk.*

1.11.13 O TRE/RN poderá solicitar o escalonamento de incidentes ao fabricante quando se tratarem de correções especiais, defeitos nos programas ou defeito em *hardware*.

1.11.14 A fornecedora da solução poderá prestar o suporte técnico dos produtos, sendo facultado a ela o escalonamento das questões para o respectivo fabricante, ficando, entretanto, a contratada responsável pelo gerenciamento do chamado e prestação de informações junto à contratante.

1.11.15 A garantia iniciará sua contagem a partir da data de emissão da nota fiscal dos *softwares*, serviços ou licenças.

1.11.16 Havendo discrepâncias entre o que está especificado no item específico e o que consta nestas condições gerais, prevalecerá o que está no item específico.

1.11.17 A fornecedora da solução deverá disponibilizar, na vigência do contrato, todas as atualizações dos *softwares* dos componentes da solução, concebidas em data posterior ao seu fornecimento, pelo período especificado no item constante do termo de referência (36 meses, a depender da garantia explicitada para o item em questão), sem qualquer ônus adicional para o contratante.

1.11.18 As atualizações incluídas devem ser do tipo "*minor release*" e "*major release*", permitindo manter todos componentes atualizados em sua última versão de *software/firmware*.

1.12 DE CAPACITAÇÃO

1.12.1 Deverá ser realizado o repasse tecnológico para a equipe técnica por meio presencial ou remotamente, com carga horária mínima de **20 (vinte) horas** e deverá abordar as informações necessárias à gerência, administração, auditoria e suporte interno da solução.

1.12.2 Além do repasse tecnológico para as equipes técnicas, deverão ser fornecidos documentos e tutoriais (em português) necessários à capacitação dos usurários finais da solução a respeito das funcionalidades da solução.

1.12.3 Ao término do repasse tecnológico, que terá o mínimo de **10 (dez) participantes**, deverão ser fornecidos atestados de participação, contendo no mínimo o nome do aluno, assunto, entidade promotora, carga horária, período de realização, ministrante e conteúdo programático.

1.13 DE EXPERIÊNCIA PROFISSIONAL DA EQUIPE QUE PROJETARÁ, IMPLEMENTARÁ E IMPLANTARÁ A SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

1.13.1 O profissional responsável pela implantação deverá apresentar documentação que ateste pelo menos **02 (dois) anos** de experiência de uso da ferramenta contratada.

1.13.1.1 Os serviços previstos objeto deste estudo preliminar deverão ser realizados por profissionais com perfis técnicos compatíveis com cada atividade, ou seja, por recursos especialistas habilitados, com base em cursos e certificações oficiais.

1.14 DE FORMAÇÃO DA EQUIPE QUE PROJETARÁ, IMPLEMENTARÁ E IMPLANTARÁ A SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

1.14.1 Não se aplica.

1.15 DE METODOLOGIA DE TRABALHO

1.15.1 Não se aplica.

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

1.16 DE SEGURANÇA DA INFORMAÇÃO

1.16.1 A fornecedora da solução deverá obedecer aos critérios, padrões, normas e procedimentos operacionais adotados pela JUSTIÇA ELEITORAL e, em especial, observar a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral, instituída através da Resolução no 23.501 de 19 de dezembro de 2016 do Tribunal Superior Eleitoral e a Política de Segurança da Informação (PSI), no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte, instituída através da Resolução n° 20/2019 de 11 de setembro de 2019, quanto aos seguintes aspectos:

1.16.1.1 Manter sigilo a respeito de quaisquer informações, dados, processos, fórmulas, códigos, cadastros, fluxogramas, diagramas lógicos, dispositivos, modelos ou outros materiais de propriedade do Tribunal Regional Eleitoral do Rio Grande do Norte aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa.

1.16.1.2 O Tribunal Regional Eleitoral do Rio Grande do Norte terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação.

1.16.1.3 Os documentos eventualmente produzidos deverão ser repassados ao TRE/RN tanto em formato não editável (*PDF*) como também em formato editável (.*DOCX* ou .*ODT*).

1.16.2 A fornecedora da solução deverá concordar que as informações a que terá acesso serão utilizadas somente nos processos envolvidos para execução do objeto contratado.

1.16.3 A fornecedora da solução se obriga a informar imediatamente ao TRE/RN qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço.

1.16.4 A solução deverá proporcionar a disponibilidade, a integridade e a segurança de todas as informações do TRE/RN por ela gerenciadas e armazenadas.

1.16.5 O acesso as ferramentas de colaboração e comunicação deverá ser feito através de conexão segura (*HTTPS*).

1.17 DE QUALIDADE

1.17.1 Não se aplica.

2 AVALIAÇÃO DE SOLUÇÕES

2.1 DISPONIBILIDADE DE SOLUÇÃO SIMILAR EM OUTRO ÓRGÃO OU ENTIDADE DA ADMINISTRAÇÃO PÚBLICA

2.1.1 Em consulta de mercado se observou que existem 03 (três) soluções capazes de prover o gerenciamento de vulnerabilidades, sem necessidade de aquisição de *hardwares* específicos, e que podem atender aos requisitos:

2.1.1.1 Utilização de ferramenta disponibilizada sob a modalidade de *softwares* livres (código aberto) ou de forma gratuita.

2.1.1.2 Utilização de ferramenta comercial com gerenciamento e armazenamento na nuvem (*On Cloud*).

2.1.1.3 Utilização de ferramenta comercial com gerenciamento e armazenamento na rede local do Tribunal (*On Premise*).

2.1.2 A tabela abaixo mostra alguns dos fornecedores da(s) solução(es):

Solução	Descrição	Fornecedor(es)
Gratuita	Ferramenta disponibilizada sob a modalidade de *softwares* livres (código aberto) ou de forma gratuita	- *OpenVas* - *Nmap*
Comercial (*On Cloud*)	Ferramenta de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseado em nuvem, com modelo de subscrição por tempo determinado	- *Qualys* - *Tenable* - *Rapid7*
Comercial (*On Premise*)	Ferramenta de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseado em gerenciamento e armazenamento na rede local do Tribunal, com modelo de subscrição por tempo determinado, ou de licença perpétua com suporte técnico por tempo determinado	- *Tenable* - *Rapid7*

2.1.3 As alternativas descritas nos itens 2.1.1.1, 2.1.1.2 e 2.1.1.3 referem-se à aquisição de *softwares* e encontram-se implantadas:

2.1.3.1 No Comando da Marinha – Dispensa de Licitação Nº 671/2018 renovação da assinatura do software Nessus da empresa *Tenable* por um período de 12 (doze) meses.

2.1.3.2 No Conselho da Justiça Federal – Processo SEI 0001989-89.2019.4.90.8000 – Pregão Eletrônico 01/2020 relata o uso só *software Rapid7*.

2.1.3.3 No Tribunal Regional Eleitoral do Paraná – Pregão Eletrônico 03/2020 – Empresa vencedora fornece a ferramenta *Qualys*.

2.1.3.4 No Banco do Estado do Rio Grande do Sul - Banrisul – Pregão Eletrônico 509/2019 – Empresa vencedora fornece o produto *Nessus* da empresa *Tenable*.

2.2 DISPONIBILIDADE SOLUÇÕES EXISTENTES NO PORTAL DO *SOFTWARE* PÚBLICO BRASILEIRO

2.2.1 Em consulta no Portal do Software Público Brasileiro não está disponível solução(ões) que atenda os requisitos.

2.3 CAPACIDADE E ALTERNATIVAS NO MERCADO DE TIC, INCLUSIVE A EXISTÊNCIA DE *SOFTWARE* LIVRE OU *SOFTWARE* PÚBLICO

2.3.1 Em consulta no mercado de TIC se observou a soluções capazes de prover o gerenciamento de vulnerabilidades, sem necessidade de aquisição de *hardwares* específicos, e que podem atender aos requisitos:

2.3.1.1 *OpenVAS* que é um *framework* de vários serviços e ferramentas que oferece uma solução de varredura e gerenciamento de vulnerabilidade.

2.3.1.2 *Nmap* que é um *software* livre que realiza *port scan,* muito utilizado para avaliar a segurança dos computadores e para descobrir serviços ou servidores em uma rede de computadores, conhecido pela sua rapidez e pelas opções que dispõe.

2.3.1.3 T*enable Nessus Vulnerability Scanner* é uma solução de avaliação de vulnerabilidades *On Cloud*.

2.3.1.3.1 Ela impede ataques de rede, identificando as vulnerabilidades e problemas de configuração que hackers usam para penetrar sua rede.

2.3.1.4 *Tenable Nessus Vulnerability Scanner* é uma solução de avaliação de vulnerabilidades *On Premisse*.

2.3.1.4.1 Ela impede ataques de rede, identificando as vulnerabilidades e problemas de configuração que *hackers* usam para penetrar sua rede.

2.3.1.5 O *Rapid7* é uma solução de gerenciamento de vulnerabilidade *On Cloud*.

2.3.1.5.1 O seu propósito é ajudar a reduzir sua exposição a ameaças, permitindo que você avalie e responda às mudanças em seu ambiente em tempo real e priorizando riscos em vulnerabilidades, configurações e controles.

2.3.1.6 O *Rapid7* é uma solução de gerenciamento de vulnerabilidade *On Premisse*.

2.3.1.6.1 O seu propósito é ajudar a reduzir sua exposição a ameaças, permitindo que você avalie e responda às mudanças em seu ambiente em tempo real e priorizando riscos em vulnerabilidades, configurações e controles.

2.3.1.7 O *Qualys Web Application Scanning (WAS)* é um serviço em nuvem que fornece rastreamento e testes automatizados de aplicativos *web* personalizados para identificar vulnerabilidades.

2.4 OBSERVÂNCIA ÀS POLÍTICAS, PREMISSAS E ESPECIFICAÇÕES TÉCNICAS DEFINIDAS PELOS MODELO NACIONAL DE INTEROPERABILIDADE DO PODER JUDICIÁRIO (MNI) E MODELO DE ACESSIBILIDADE DE GOVERNO ELETRÔNICO (E-MAG)

2.4.1 A solução a ser implantada não tem por finalidade a comunicação com outros órgãos do Poder Judiciário, portanto, não se aplica a observância ao Modelo Nacional de Interoperabilidade MNI.

2.4.2 A solução a ser implantada será acessível somente a determinados servidores do quadro deste regional, portanto, não se aplica a observância ao Modelo de Acessibilidade de Governo Eletrônico E-MAG.

2.5 OBSERVÂNCIA AOS REQUISITOS ESTABELECIDOS PELA RESOLUÇÃO CNJ Nº 211/2015 E ALTERAÇÕES POSTERIORES, NA CONTRATAÇÃO DE SERVIÇOS DE DESENVOLVIMENTO E DE SUSTENTAÇÃO DE SISTEMAS DE INFORMAÇÃO

2.5.1 Não se aplica.

2.6 ADERÊNCIA ÀS REGULAMENTAÇÕES DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRAS (ICP-BRASIL), QUANDO HOUVER NECESSIDADE DE UTILIZAÇÃO DE CERTIFICADO DIGITAL, OBSERVADA A LEGISLAÇÃO SOBRE O ASSUNTO

2.6.1 Não se aplica.

2.7 OBSERVÂNCIA ÀS ORIENTAÇÕES, PREMISSAS E ESPECIFICAÇÕES TÉCNICAS E FUNCIONAIS DEFINIDAS PELO MODELO DE REQUISITOS PARA SISTEMAS INFORMATIZADOS DE GESTÃO DE PROCESSOS E DOCUMENTOS DO PODER JUDICIÁRIO (MOREQ-JUS), DO CONSELHO NACIONAL DE JUSTIÇA – CNJ E PELO E-ARQ (NORMAS E PADRÕES DE ARQUIVOLOGIA)

2.7.1 Não se aplica.

2.8 ORÇAMENTO ESTIMADO QUE EXPRESSE A COMPOSIÇÃO DE TODOS OS CUSTOS UNITÁRIOS RESULTANTES DOS ITENS A SEREM CONTRATADOS, ELABORADO COM BASE EM PESQUISA FUNDAMENTADA DE PREÇOS, COMO OS PRATICADOS NO MERCADO DE TIC EM CONTRATAÇÕES SIMILARES REALIZADAS POR ÓRGÃOS OU ENTIDADES DA ADMINISTRAÇÃO PÚBLICA, ENTRE OUTROS PERTINENTES

2.8.1 Em consulta realizada em âmbito nacional para uma prévia comparação de custos, se obteve o seguinte:

Item	Fornecedor	Descrição/ Modelo	Quant. Prevista	Quant. Registrada	Valor Unitário	Valor Total
2.8.1.1	Comunidades	*Software* livre OpenVas	0	0	R$ 0,00	R$ 0,00
		Software livre *Nmap*	0	0	R$ 0,00	R$ 0,00
Total						**R$ 0,00**

Item	Fornecedor	Descrição/ Modelo	Quant. Prevista	Quant. Registrada	Valor Unitário	Valor Total
2.8.1.2	Qualys (*On Cloud*)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando, no mínimo, **250 (duzentos e cinquenta) endereços *IPs***, por **36 (trinta e seis) meses** de uso e suporte do fabricante	1	1	R$ 137.826,00	R$ 137.826,00
		Licenciamento para solução de análise dinâmica em aplicações *Web*, pacote para, no mínimo, **05 (cinco) domínios** (*FQDN*), por **36 (trinta e seis) meses** de uso e suporte do fabricante	1	1	R$ 59.970,00	R$ 59.970,00
		Instalação e configuração	1	1	R$ 6.890,00	R$ 6.890,00
		Repasse tecnológico, com período mínimo de **20 (vinte) horas**	1	1	R$ 4.500,00	R$ 4.500,00
		04 (quatro) horas de serviço especializado	0	50	R$ 1.250,00	R$ 0,00
Total						**R$ 209.186,00**

Item	Fornecedor	Descrição/ Modelo	Quant. Prevista	Quant. Registrada	Valor Unitário	Valor Total
2.8.1.3	Rapid7 (*On Cloud*)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando, no mínimo, **250 (duzentos e cinquenta) endereços *IPs***, por **36 (trinta e seis) meses** de uso e suporte do fabricante	1	1	R$ 155.375,00	R$ 155.375,00
		Licenciamento para solução de análise dinâmica em aplicações *Web*, pacote para, no mínimo, **05 (cinco) domínios** (*FQDN*), por **36 (trinta e seis) meses** de uso e suporte do fabricante	1	1	R$ 246.622,00	R$ 246.622,00
		Instalação e configuração e repasse Tecnológico com período mínimo de **20 (vinte) horas**	1	1	R$ 38.000,00	R$ 38.000,00
		Repasse tecnológico, com período mínimo de **20 (vinte) horas**	1	1	R$ 10.000,00	R$ 10.000,00
		Banco de **04 (quatro) horas** técnicas (*on demand*) 100% REMOTO em regime de atendimento 8x5	0	1	R$ 1.000,00	R$ 1.000,00
Total						**R$ 450.997,00**

Item	Fornecedor	Descrição/ Modelo	Quant. Prevista	Quant. Registrada	Valor Unitário	Valor Total
2.8.1.4	*Tenable* (*On Cloud*)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando, no mínimo, **250 (duzentos e cinquenta) endereços *IPs***, por **36 (trinta e seis) meses** de uso e suporte do fabricante	1	1	R$ 158.250,00	R$ 158.250,00
		Licenciamento para solução de análise dinâmica em aplicações *Web*, pacote para, no mínimo, **05 (cinco) domínios** (*FQDN*), por **36 (trinta e seis) meses** de uso e suporte do fabricante	1	1	R$ 64.710,00	R$ 64.710,00
		Instalação e configuração e repasse Tecnológico com período mínimo de **20 (vinte) horas**	1	1	R$ 11.322,00	R$ 11.322,00
		Repasse tecnológico, com período mínimo de **20 (vinte) horas**	1	1	R$ 8.342,00	R$ 8.342,00
		04 (quatro) horas de serviço especializado	0	50	R$ 0,00	R$ 0,00
		Total				**R$ 242.624,00**

Item	Fornecedor	Descrição/ Modelo	Quant. Prevista	Quant. Registrada	Valor Unitário	Valor Total
2.8.1.5	*Rapid7* (*On Premise*)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo **250 (duzentos e cinquenta) endereços IPs**, por **36 (trinta e seis) meses** de uso e suporte do fabricante	1	1	R$ 155.375,00	R$ 155.375,00
		Licenciamento para solução de análise dinâmica em aplicações *Web*, pacote para no mínimo **05 (cinco) domínios** (FQDN), por **36 (trinta e seis) meses** de uso e suporte do fabricante	1	1	R$ 369.933,75	R$ 369.933,75
		Instalação e configuração e repasse Tecnológico com período mínimo de **20 (vinte) horas**	1	1	R$ 38.000,00	R$ 38.000,00
		Repasse Tecnológico com período mínimo de **20 (vinte) horas**	1	1	R$ 10.000,00	R$ 10.000,00
		Banco de **04 (quatro) horas** técnicas (*on demand*) 100% REMOTO em regime de atendimento 8x5	0	1	R$ 1.000,00	R$ 1.000,00
		Total				**R$ 574.308,75**

Item	Fornecedor	Descrição/ Modelo	Quant. Prevista	Quant. Registrada	Valor Unitário	Valor Total
2.8.1.6	*Tenable* (*On Premise*)	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo **250 (duzentos e cinquenta) endereços *IPs***, por **36 (trinta e seis) meses** de uso e suporte do fabricante	1	1	R$ 145.650,96	R$ 145.650,96
		Licenciamento para solução de análise dinâmica em aplicações Web, pacote para no mínimo **05 domínios** (**FQDN**), por **36 (trinta e seis) meses** de uso e suporte do fabricante	1	1	R$ 0,00	R$ 0,00
		Instalação e configuração	1	1	R$ 11.322,00	R$ 11.322,00
		Repasse Tecnológico com período mínimo de **20 (vinte) horas**	1	1	R$ 8.342,00	R$ 8.342,00
		04 (quatro) horas de Serviço Especializado	0	50	R$ 0,00	R$ 0,00
		Total				**R$ 165.314,96**

3 ESCOLHA E JUSTIFICATIVA DA SOLUÇÃO

3.1 **A solução escolhida foi a alternativa descrita:**

3.1.1 No **item 2.8.1.6** fornecida pela empresa *Tenable*.

3.1.1.1 Esta solução é baseada no gerenciamento em rede local do TRE/RN, possui o menor preço dentre os itens apresentados e atende todos os requisitos já elencados.

3.2 **Justificativa da escolha:**

3.2.1 Após avaliarmos as soluções contidas no **item 2.8.1**, podemos justificar a nossa escolha com base nos seguintes argumentos:

3.2.1.1 As soluções contidas no **item 2.8.1.1** são baseadas em *software* livre e atendem apenas parte da necessidade, pois a utilização desse cenário implica em não contar com suporte técnico especializado.

3.2.1.1.1 Além disso, a atualização da base de vulnerabilidades e falhas não possui a mesma frequência de cenários com softwares pagos.

3.2.1.1.2 Outro ponto desfavorável ao uso desses *softwares* é que os relatórios fornecidos pelas ferramentas não apresentam rastreabilidade das atividades já realizadas nos ativos e sistemas.

3.2.1.2 As soluções contidas nos **itens 2.8.1.2, 2.8.1.3** e **2.8.1.4** são baseadas em nuvem (*cloud computing*) e apresentam facilidade de gerenciamento, valor de aquisição adequado e facilidade nas atualizações da solução que serão todas feitas pelo fabricante.

3.2.1.2.1 Todos os requisitos de funcionalidades do projeto são atendidos por esse cenário.

3.2.1.2.2 As soluções analisadas *Qualys* (*VM* e módulo *WAS*), *Tenable* (*Tenable.io* e módulo *WAS*) e *Rapid7* (*IVM* e módulo *IAS*) conseguem fazer o gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações *Web*.

3.2.1.2.3 Porém como os dados armazenados pela ferramenta (vulnerabilidades dos ativos de TIC) são muito sensíveis não é recomendável estarem armazenados em nuvem pública.

3.2.1.3 As soluções contidas nos **itens 2.8.1.5** e **2.8.1.6** são baseadas no gerenciamento em rede local do TRE/RN (*On Premise*).

3.2.1.3.1 A solução fornecida pela *Tenable* apresenta um valor de aquisição adequado e menor do que a solução que consta no **item 2.8.1.4** (*On Cloud*).

3.2.1.3.1.1 Apesar do **item 2.8.1.6** (*On Premise*) trazer o trabalho de atualização para a equipe de infraestrutura de rede, ela possui um menor risco de vazamento de dados sensíveis que são as vulnerabilidades dos ativos de TIC do Tribunal, pois os mesmos serão armazenados na rede local do Tribunal e não em nuvem pública.

3.2.1.3.1.2 Todas os requisitos de funcionalidades do projeto também são atendidos por esse cenário.

3.2.1.3.1.3 As soluções analisadas *Tenable* e *Rapid7* conseguem fazer o gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações *Web*.

3.2.1.3.1.4 Outro ponto favorável ao **item 2.8.1.6** fornecido pela *Tenable* é o fato de que após o término do suporte, a STIE continuará a ter acesso a ferramenta embora sem o direito de recebimento de atualizações de versão e de novas vulnerabilidades.

3.2.1.4 **Atualmente está em curso no Tribunal Regional Eleitoral da Paraíba, com apoio de outros Regionais, um registro de preços para a contratação de ferramenta de gestão de vulnerabilidades, que atende a todos os requisitos elencados neste estudo, onde o processo está bem avançado e que se configuraria a solução mais vantagosa, caso o TRE/RN optasse por participar do referido registro de preços.**

3.3 **A solução está alinhada:**

3.3.1 Às necessidades de negócio e requisitos tecnológicos.

3.3.2 **Necessidade de alcance dos seguintes objetivos estratégicos, elencados no:**

3.3.2.1 **Plano Estratégico da Justiça Eleitoral do RN 2016-2020 (PEJERN):**

3.3.2.1.1 Aprimorar a infraestrutura, a gestão e a governança de Tecnologia da Informação e Comunicação (TIC) – Objetivo Estratégico nº 9 (nove).

3.3.2.2 **Plano Estratégico de Tecnologia da Informação e Comunicação 2016-2020 (PETIC):**

3.3.2.2.1 Aperfeiçoar a segurança da informação e comunicação – Objetivo Estratégico nº 05 (cinco). .

3.3.2.2.2 Primar pela satisfação dos usuários de Tecnologia da Informação e Comunicação (TIC) – Objetivo Estratégico nº 06 (seis).

3.4 **A solução escolhida permitirá:**

3.4.1 Identificar as vulnerabilidades dos ativos de tecnologia da informação utilizados no TRE/RN.

3.4.2 Definir o grau de risco de cada ativo de acordo com as áreas de negócio.

3.4.3 Priorizar as ações necessárias à mitigação de riscos e correção das vulnerabilidades.

3.5 **A solução é composta por *softwares*:**

3.5.1 Atualmente existe a necessidade de aquisição de ferramenta de gestão de vulnerabilidades, conforme abaixo:

Item	Descrição	Tipo
1	Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando, no mínimo, **250 (duzentos e cinquenta) endereços IPs**, por **36 (trinta e seis) meses** de uso e suporte do fabricante	*Tenable.sc Vulnerability Management*
2	Licenciamento para solução de análise dinâmica em aplicações *Web*, pacote para, no mínimo, **05 (cinco) domínios** (FQDN), por **36 (trinta e seis) meses** de uso e suporte do fabricante	*Tenable Web Application Scanning*

3	Instalação e configuração	-
4	Repasse tecnológico	Por um período mínimo de **20 (vinte) horas**
5	Suporte técnico	**04 (quatro) horas** de serviço especializado

3.6 **Os valores estimados estão descritos no item 2.8.1.**

3.7 **Os benefícios gerados são:**

3.7.1 Reduzir o nível de risco do ambiente de TIC por meio da correção das vulnerabilidades identificadas.

3.7.2 Proteger a informação e os ativos de tecnologia da informação utilizados no TRE/RN.

3.7.3 Garantir a disponibilidade dos sistemas que sustentam os serviços essenciais e a continuidade dos serviços oferecidos e uso das aplicações desenvolvidas e utilizadas pela Justiça Eleitoral.

3.7.4 Manter uma infraestrutura tecnológica compatível com as necessidades do TRE/RN, objetivando a busca contínua pela melhoria da qualidade e o padrão de excelência na prestação de serviços ao público interno e externo.

3.8 Relação Demanda Prevista x Quantidade de Bens Pretendidos (memória de cálculo):

3.8.1 Atualmente, considerando o aspecto orçamentário, a necessidade será atendida pela contratação de licenças do(s) seguinte(s) *software(s)*, na(s) quantidade(s) indicada(s):

Descrição	**Quant. Atual**	**Quant. Necessária (Projeção)**	**Quant. para Aquisição**
Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando, no mínimo, **250 (duzentos e cinquenta) endereços *IPs***, por **36 (trinta e seis) meses** de uso e suporte do fabricante.	0	01	01
Licenciamento para solução de análise dinâmica em aplicações Web, pacote para, no mínimo, **05 (cinco) domínios** (*FQDN*), por **36 (trinta e seis) meses** de uso e suporte do fabricante.	0	01	01

4 NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE

4.1 Não existe necessidade de adequação do ambiente para a execução contratual.

II – SUSTENTAÇÃO DA CONTRATAÇÃO

5 DEFINIÇÃO DE RECURSOS HUMANOS E MATERIAIS

5.1 IDENTIFICAÇÃO DOS RECURSOS HUMANOS NECESSÁRIOS À IMPLANTAÇÃO DA SOLUÇÃO

5.1.1 Representante Técnico na licitação

5.1.1.1 Francisco de Assis Paiva Leal

5.1.1.2 Responsabilidades:

5.1.1.2.1 Apoiar o pregoeiro durante todo processo licitatório

5.1.1.2.2 Responder os questionamentos dos licitantes durante o certame.

5.1.2 Técnico Segurança da Informação

5.1.2.1 Francisco de Assis Paiva Leal.

5.1.2.2 Responsabilidades:

5.1.2.2.1 Analisar se todos requisitos técnicos exigidos foram atendidos durante o processo de entrega da solução.

5.1.2.2.2 Monitorar a solução no estagio de produção.

5.1.2.2.3 Acionar o suporte de garantia quando necessário.

5.1.3 Equipe de Recebimento

5.1.3.1 Seção de Segurança da Informação

5.1.3.2 Responsabilidades:

5.1.3.2.1 Monitorar a entrega da solução quanto ao prazo e os requisitos técnicos e administrativos.

5.2 IDENTIFICAÇÃO DOS RECURSOS MATERIAIS NECESSÁRIOS À IMPLANTAÇÃO DA SOLUÇÃO

5.2.1 Não foi identificada a necessidade de recursos materiais adicionais para garantir a implantação da solução.

5.3 IDENTIFICAÇÃO DOS RECURSOS HUMANOS NECESSÁRIOS À CONTINUIDADE DA SOLUÇÃO

5.3.1 Não foi identificada a necessidade de recursos humanos adicionais para garantir a continuidade da solução.

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

5.4 IDENTIFICAÇÃO DOS RECURSOS MATERIAIS NECESSÁRIOS À CONTINUIDADE DA SOLUÇÃO

5.4.1 Não foi identificada a necessidade de recursos materiais adicionais para garantir a continuidade da solução.

5.5 IDENTIFICAÇÃO DA EQUIPE DE APOIO À LICITAÇÃO NECESSÁRIA À CONTINUIDADE DA SOLUÇÃO

5.5.1 A equipe de apoio à licitação necessária à continuidade da solução será composta por:

Nome do Servidor	Unidade de Lotação	Papel desempenhado
Francisco de Assis Paiva Leal	SSI/COINF/STIE	Integrante Técnico
Marat Soares Teixeira	SELIC/COLIC/SAOF	Integrante Administrativo
Denílson Bastos da Silva	SSI/COINF/STIE	Auxiliar Técnico
Helder Jean Brito da Silva	SSI/COINF/STIE	Auxiliar Técnico
Daniel César Gurgel Coelho Ponte	SRI/COINF/STIE	Auxiliar Técnico
João Paulo de Araújo Bezerra	SRI/COINF/STIE	Auxiliar Técnico

6 DEFINIÇÃO DAS ATIVIDADES DE TRANSIÇÃO E ENCERRAMENTO DA CONTRATAÇÃO

6.1 Não se aplica.

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

7 ELABORAÇÃO DE ESTRATÉGIA DE INDEPENDÊNCIA

7.1 TRANSFERÊNCIA DE CONHECIMENTO TECNOLÓGICO

7.1.1 Não se aplica.

7.2 DIREITOS DE PROPRIEDADE INTELECTUAL E AUTORAIS

7.2.1 Não se aplica.

7.3 DOCUMENTAÇÃO E AFINS PERTINENTES À TECNOLOGIA DE CONCEPÇÃO, MANUTENÇÃO, ATUALIZAÇÃO E CÓDIGO FONTE

7.3.1 Não se aplica.

III – ANÁLISE DE RISCOS

8 IDENTIFICAÇÃO DOS RISCOS

8.1 RISCOS DO PROCESSO DE CONTRATAÇÃO

Risco	**8.1.1 Indisponibilidade Orçamentária**	**Probabilidade:**	**MÉDIA**
Item	Dano		Impacto:
1	Não contratação imediata da solução		**ALTO**
2	Atraso no cronograma		**MÉDIO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Verificar e confirmar previamente disponibilidade orçamentária para a contratação da solução pretendida		STIE
2	Encaminhar em tempo hábil proposta de dotação orçamentária ao Órgão Ordenador de Despesas com previsão e prazo para a contratação da solução		STIE
Item	**Corretiva**		**Responsável**
1	Solicitar o remanejamento de recursos para atender temporariamente o serviço objeto do Termo de Referência		STIE

Risco	8.1.1 **Atraso no Trâmite Processual**	**Probabilidade:**	**MÉDIA**
Item	**Dano**		**Impacto:**
1	Atraso na contratação da solução		**MÉDIO**
2	Atraso no cronograma		**MÉDIO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Finalizar o Termo de Referência e documentos acessórios respeitando o cronograma previamente definido		Equipe de Planejamento da Contratação
2	Comunicar à Administração da criticidade do objeto contratado e da necessidade de agilidade na análise dos documentos e na tramitação do processo administrativo		STIE
Item	**Corretiva**		**Responsável**
1	Comunicar à Administração sobre a paralisação do processo durante a tramitação e solicitar prioridade na análise visando à conclusão do processo administrativo		STIE

Risco	8.1.2 **Impugnação Procedente**	**Probabilidade:**	**BAIXA**
Item	**Dano**		**Impacto:**
1	Interrupção do processo de contratação		**ALTO**
2	Atraso no cronograma		**ALTO**
3	Frustração da contratação		**ALTO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Elaboração de Estudos Preliminares e Termo de Referências consistentes que permitam assegurar a contratação		Equipe de Planejamento da Contratação
2	Revisar o Termo de Referência e certificar que o mesmo não possua cláusulas que restrinjam, sem a devida justificativa técnica, a participação de interessados ou que, de alguma forma, deixem um licitante em situação privilegiada para concorrer		Equipe de Planejamento da Contratação
3	Submeter, para análise, o Termo de Referência à Administração		Equipe de Planejamento da Contratação
4	Atendimento imediato por parte do suporte técnico a fim de responder, tempestivamente, os pedidos de esclarecimentos e impugnações apresentadas		Equipe de Planejamento da Contratação
Item	**Corretiva**		**Responsável**
1	Adequação do Termo de Referência, corrigindo os itens que foram motivos de impugnação, para viabilizar a reabertura do certame.		Equipe de Planejamento da Contratação
2	Promover a reabertura da licitação		Área Administrativa

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Risco	8.1.3 **Licitação Frustrada (Deserta/Fracassada)**	**Probabilidade:**	**BAIXA**
Item	**Dano**		**Impacto:**
1	Interrupção do processo de contratação		**ALTO**
2	Atraso no cronograma		**ALTO**
3	Frustração da contratação		**ALTO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Promover análise de mercado com o objetivo de elencar as empresas que prestam serviço do objeto		Equipe de Planejamento da Contratação
2	Dar a devida publicidade ao certame licitatório		Área Administrativa
3	Evitar exigências técnicas demasiadamente restritivas e desnecessárias		Equipe de Planejamento da Contratação
4	Mensurar o preço global do serviço a ser contratado através de estudo minucioso, com pesquisa de preços na Internet, bem como com prestadores de serviço do ramo		Equipe de Planejamento da Contratação
Item	**Corretiva**		**Responsável**
1	Adequação do Termo de Referência para a realização de novo certame		Equipe de Planejamento da Contratação
2	Promover nova licitação		Área Administrativa
3	Pesquisa de Preços, caso necessário		Equipe de Planejamento da Contratação
4	Contratação Direta		Área Administrativa

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

Risco	8.1.4 **Licitação Anulada**	**Probabilidade:**	**BAIXA**
Item	**Dano**		**Impacto:**
1	Interrupção do processo de contratação		**ALTO**
2	Atraso no cronograma		**ALTO**
3	Frustração da contratação		**ALTO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Na elaboração do Termo de Referência observar se não existe vício de legalidade		Equipe de Planejamento da Contratação
2	Observar adequada publicidade da licitação		Área Administrativa
Item	**Corretiva**		**Responsável**
1	Adequação das exigências normativas sobre o objeto/procedimento licitatório		Equipe de Planejamento da Contratação
2	Promover a publicidade adequada à modalidade de licitação escolhida		Área Administrativa

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40

8.2 RISCOS DA SOLUÇÃO DE TID (GESTÃO E EXECUÇÃO CONTRATUAL)

Risco	**8.2.1 Solução considerada inadequada pela área requisitante**	**Probabilidade:**	**BAIXA**
Item	**Dano**		**Impacto:**
1	Insatisfação dos usuários dos serviços de TIC		**ALTO**
2	Não utilização da solução		**ALTO**
3	Necessidade de nova avaliação da solução		**MÉDIO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Envolver o usuário/unidade requisitante na participação em todas as fases da contratação		STIE e SAOF
2	Nomear servidores experientes e capacitados para executar a fase de levantamento de requisitos da solução de TIC		STIE
Item	**Corretiva**		**Responsável**
1	Nomear nova Equipe de Planejamento da Contratação, substituindo a atual, para a elaboração de novo Termo de Referência visando a contratação de solução de TIC adequada a solicitação da área demandante		Área Administrativa
2	Nomear equipe ou realocar servidores do TRE/RN com o objetivo de auxiliar ou assumir, provisoriamente, a operação dos serviços prestados pela equipe da fornecedora da solução		STIE
3	Refazer o levantamento de requisitos junto ao usuário/unidade requisitante		STIE
4	Proceder com as alterações necessárias, na medida do possível, na solução de TIC fornecedora da solução, com objetivo de readequar e reimplantar a solução		STIE

Risco	**8.2.2 Não cumprimento do prazo de entrega do *software***	**Probabilidade:**	**BAIXA**
Item	Dano		Impacto:
1	Atraso na instalação da(s) licença(s)		**BAIXO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Consultar as empresas do ramo sobre adequação do prazo de entrega do software		STIE
2	Acompanhar rigorosamente junto à empresa o andamento da operação de entrega		Área Administrativa
Item	**Corretiva**		**Responsável**
1	Solicitar o fornecedor para a entrega imediata		Área Administrativa
2	Verificar as sanções cabíveis no caso do não cumprimento do prazo de entrega		Área Administrativa

Risco	**8.2.2 Entrega de software incompatível (especificações)**	**Probabilidade:**	**BAIXA**
Item	Dano		Impacto:
1	Ineficácia na execução dos serviços prestados pelo órgão		**ALTO**
Ações de Prevenção/Contingência e Responsáveis			
Item	**Preventiva**		**Responsável**
1	Verificar se o software está de acordo com as especificações mínimas exigidas no ato de entrega para fins de ateste provisório		STIE
Item	**Corretiva**		**Responsável**
1	Solicitar o fornecedor para a substituição do software incompatível		STIE
2	Informar o gestor da contratação sobre problemas contratuais de garantia		STIE

IV – CONCLUSÃO DOS ESTUDOS PRELIMINARES

9 DECLARAÇÃO DE VIABILIDADE

Em conformidade com o disposto no Manual de Contratações de Tecnologia da Informação e Comunicação, subitem 4.1.1.11, DECLARAMOS a viabilidade da contratação, com base no estudo realizado.

Natal/RN, *(datação eletrônica)*

Equipe de Planejamento da Contratação		
Integrante Demandante	**Integrante Técnico**	**Integrante Administrativo**
(assinado eletronicamente)	(assinado eletronicamente)	(assinado eletronicamente)
Denilson Bastos da Silva	**Francisco de Assis Paiva Leal**	**Marat Soares Teixeira**
SSI/COINF/STIE	SSI/COINF/STIE	SELIC/COLIC/SAOF

DENILSON BASTOS DA SILVA:20024241 Assinado de forma digital por DENILSON BASTOS DA SILVA:20024241 Dados: 2020.10.23 19:21:28 -03'00'

FRANCISCO DE ASSIS PAIVA LEAL:92440776 Assinado de forma digital por FRANCISCO DE ASSIS PAIVA LEAL:92440776 Dados: 2020.10.23 18:57:47 -03'00'

Documento assinado digitalmente por:		
FRANCISCO DE A. PAIVA LEAL:92440776 23/10/2020 18:57:47	DENILSON BASTOS DA SILVA:20024241 23/10/2020 19:21:28	Marat Soares Teixeira 23/10/2020 19:41:40